UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

George Webb Sweigert,
Plaintiff,
-against-

CASE: 2: 22-cv-02788-LGS

Jason Goodman,
D/B/A CrowdSource The Truth
Defendant.

Pro Se Intervenor
D. G. SWEIGERT, C/O
AMERICA'S RV
MAILBOX, PMB 13339
514 Americas Way, Box
Elder, SD 57719
Spoliation-notice@mailbox.org

Defendant Pro Se
JASON GOODMAN,
CROWDSOURCE THE TRUTH
252 7th Avenue, #6
New York, New York 10001
(323) 744-7594
truth@crowdsourcethetruth.org

Plaintiff Pro Se
GEORGE WEBB SWEIGERT
1671 W. STEARNS ROAD, SUITE E
TEMPERANCE, MI 48182
503-919-0748
Georg.webb@gmail.com

PROPOSED INTERVENOR'S SUPPLEMENT TO ECF NO. 49

I hereby attest that the foregoing was transmitted on June First, 2022 (6/1/22) under the penalties of perjury.

D. G. SWEIGERT, C/O
AMERICA'S RV MAILBOX, PMB 13339
514 Americas Way, Box Elder, SD 57719

PROPOSED INTERVENOR'S SUPPLEMENT TO ECF NO. 49

I hereby attest that the attached public documents are true and accurate artifacts under the penalties of perjury.

D. G. SWEIGERT, C/O
AMERICA'S RV MAILBOX, PMB 13339
514 Americas Way, Box Elder, SD 57719

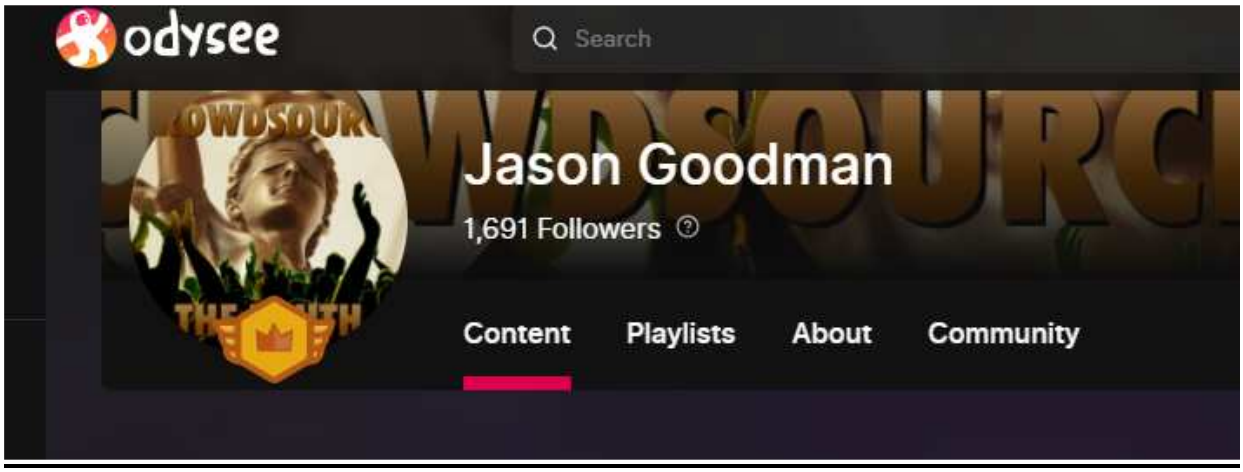
The foregoing document has been sent via e-mail message to:

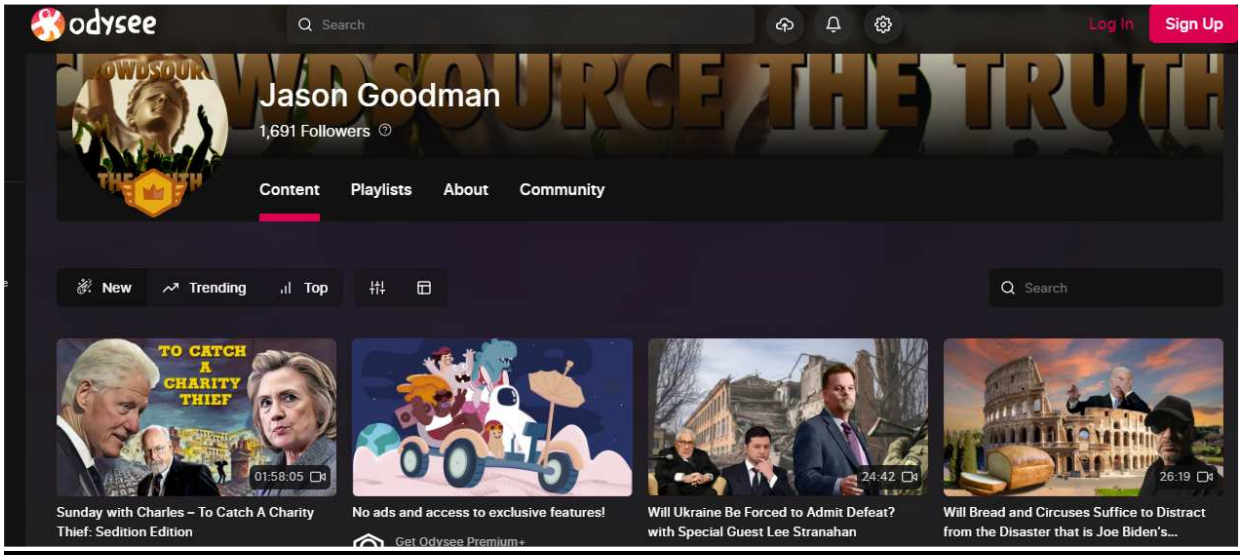
georg.webb@gmail.com and truth@crowdsourcethetruth.org on June First, 2022, (6/1/2022) sworn under penalties of perjury

D. G. SWEIGERT, C/O

EXHIBIT ONE

https://odysee.com/@Crowdsourcethetruth:d





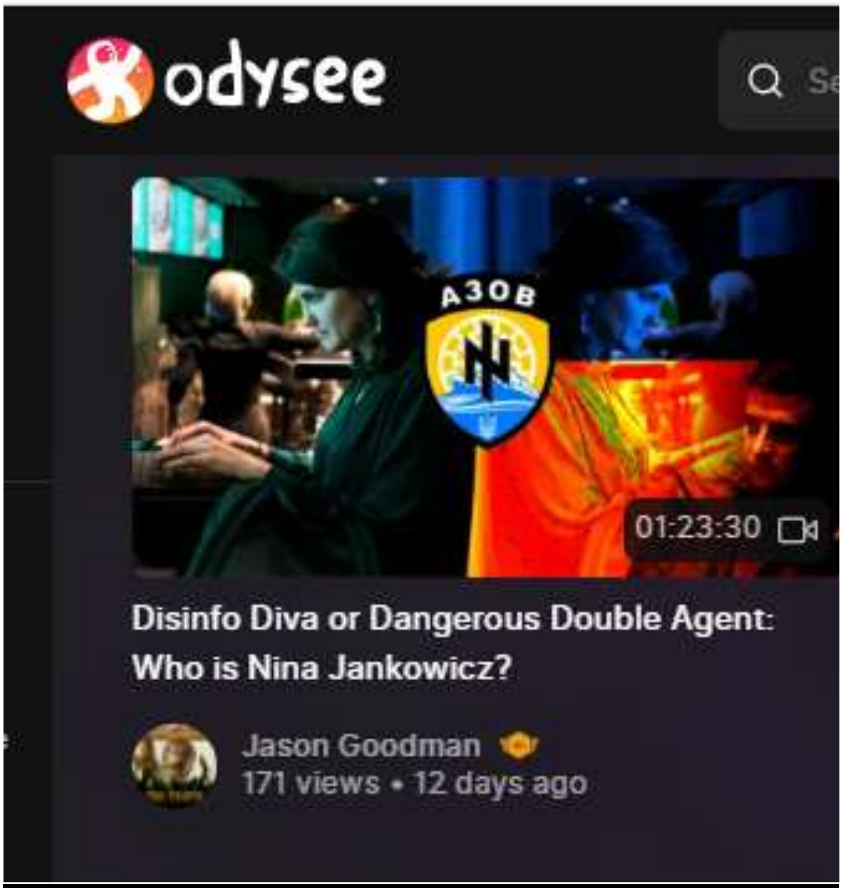

odysee
A3OB
01:23:30
Disinfo Diva or Dangerous Double Agent:
Who is Nina Jankowicz?
Jason Goodman
171 views • 12 days ago

EXHIBIT TWO

https://odysee.com/@Crowdsourcethetruth:d/2022-05-16-20-00-03-Live:9

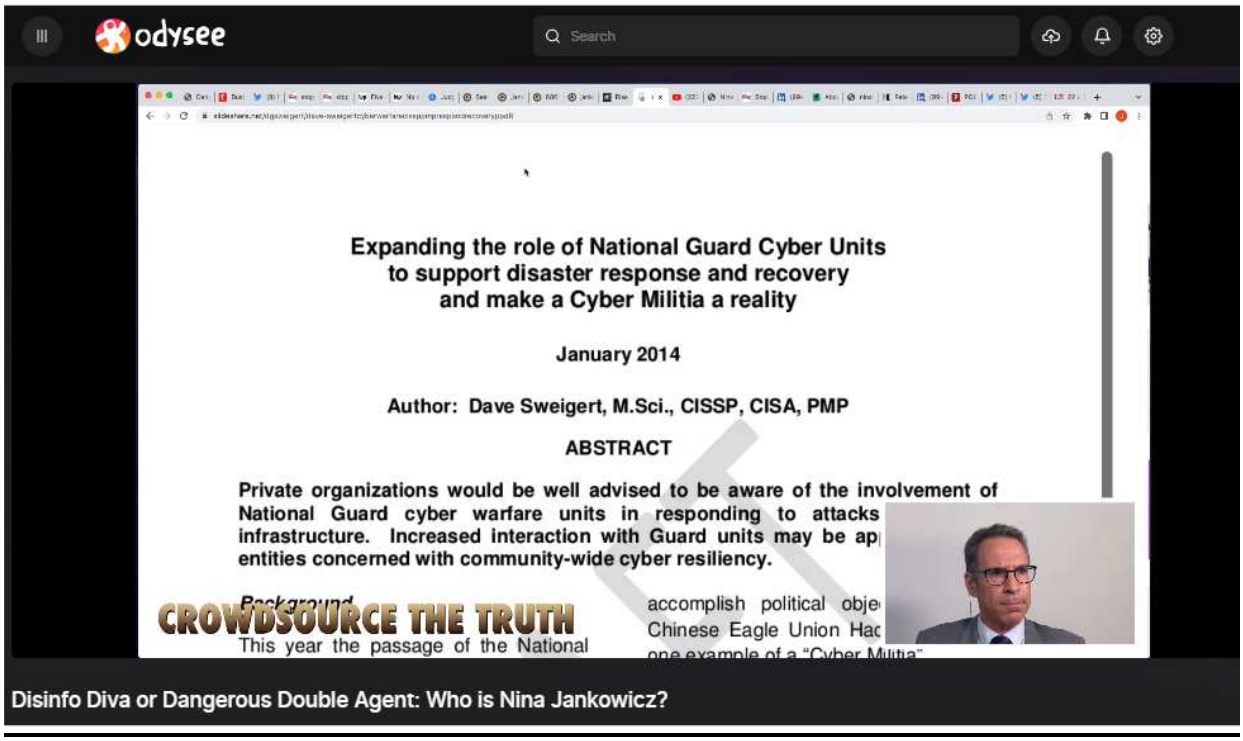
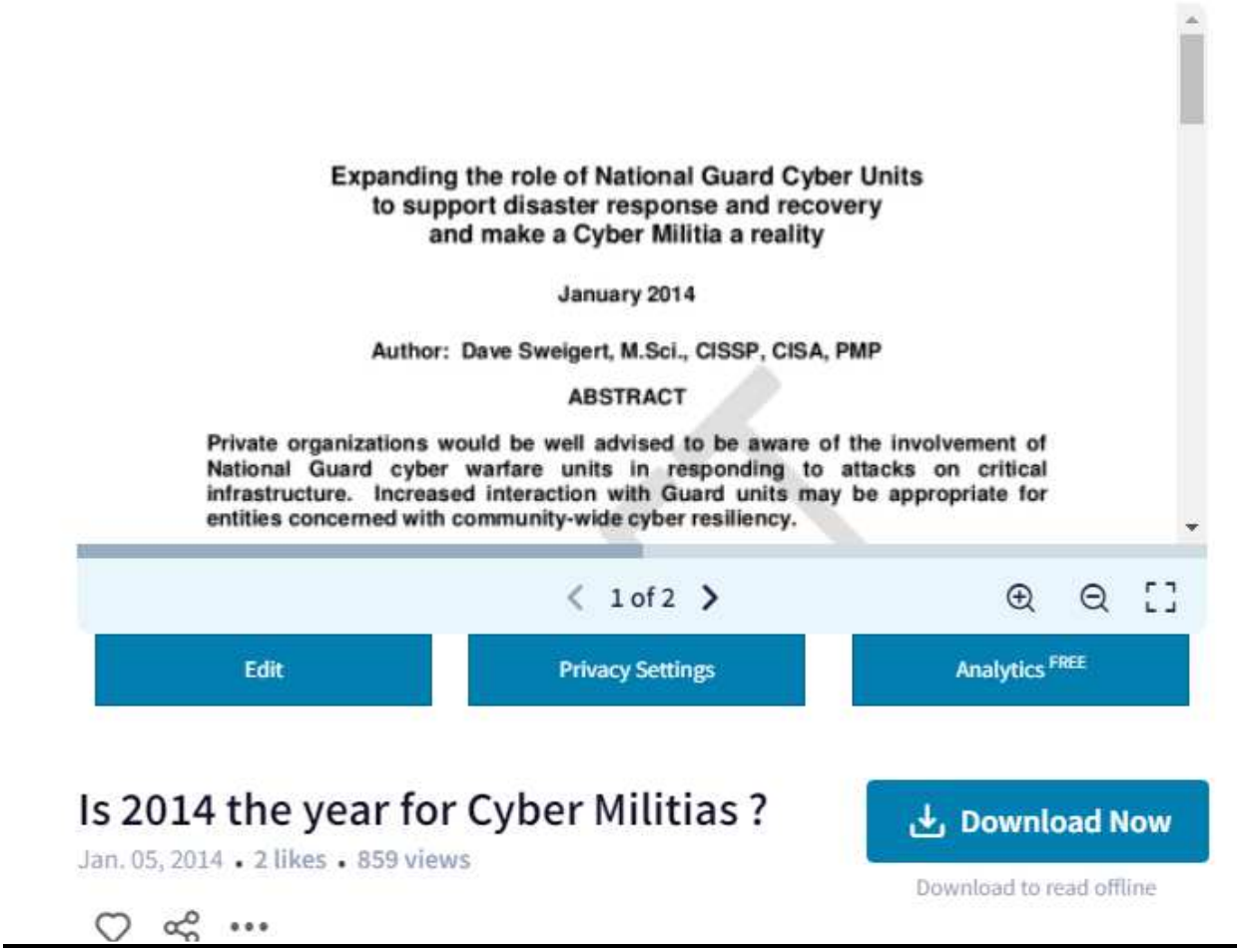

odysee
Search
Expanding the role of National Guard Cyber Units
to support disaster response and recovery
and make a Cyber Militia a reality
January 2014
Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP
ABSTRACT
Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks
infrastructure. Increased interaction with Guard units may be ap
entities concerned with community-wide cyber resiliency.
CROWDSOURCE THE TRUTH
This year the passage of the National
accomplish political obje
Chinese Eagle Union Hac
Disinfo Diva or Dangerous Double Agent: Who is Nina Jankowicz?

EXHIBIT THREE

https://www.slideshare.net/dgsweigert/dave-sweigertcyberwarfarecissppmprespondrecoveryppd8



Expanding the role of National Guard Cyber Units
to support disaster response and recovery
and make a Cyber Militia a reality

January 2014

Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP

ABSTRACT

Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks on critical infrastructure. Increased interaction with Guard units may be appropriate for entities concerned with community-wide cyber resiliency.

1 of 2

Edit Privacy Settings Analytics FREE

Is 2014 the year for Cyber Militias ?

Jan. 05, 2014 • 2 likes • 859 views

Download Now

Download to read offline

Expanding the role of National Guard Cyber Units to support disaster response and recovery and make a Cyber Militia a reality

January 2014

Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP

ABSTRACT

Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks on critical infrastructure. Increased interaction with Guard units may be appropriate for entities concerned with community-wide cyber resiliency.

Background

This year the passage of the National Defense Authorization Act (NDAA) by the U.S. Congress (used to supply the Pentagon with another year's budget) came with cybersecurity strings attached – the requirement for a comprehensive domestic cyber warfare assessment of how the National Guard would support defensive cyber warfare operations and support missions of the U.S. Department of Homeland Security.

In sum, there is likely to be a new cybersecurity player in the Critical Infrastructure – Key Resources (CIKR) arena, the National Guard.

Is this the creation of a Cyber Militia?

Cyber Militias: these are non-state sponsored collections of volunteers that can act in a militant offensive and defensive manner in cyber space. These groups can be loosely organized and operate with technical know-how to accomplish political objectives. The Chinese Eagle Union Hacker Group is one example of a "Cyber Militia".

Attacks launched by such groups that breach network cybersecurity are classified as "cyber warfare" by the Pentagon. Doomsday scenarios predict everything from massive failures of the power grid to the destruction of medical data as a consequence of an act of cyber war by such groups, creating "cyber anxiety".

Many observers have suggested that the language of the 2014 NDAA is a Dr. Strangelovian attempt to "close the cyber militia gap" and keep up with the creation of such militias in Russia, Iran, and North Korea.

Cyber Warfare: Both the National Guard Bureau (NGB) and the National Governor's Association (NGA) have openly endorsed the idea of Guard units engaged in civilian defensive cyber warfare operations.

Domestic Cyber Missions

Until now, the number of Guard units involved in civilian cybersecurity events could be counted with one hand. Examples:

Prior to the 2010 Winter Olympics the network supporting Washington State's Division of Motor Vehicles (DMV) was assessed by a Guard cyber warfare unit. Networks supporting the 2012 Presidential Inauguration were protected by such units and State networks supporting Emergency Management (E.M.) activities have also been accessed by these groups.

Such activities fall within the **National Prevention Framework** "cybersecurity" category as a **PROTECTION** capability.

With the desire of Congress to "close the gap" the scope of such support by Guard units in domestic cyber missions could be expanding. Cascading consequences created by a cyber event are addressed within the **National Response Framework** as a **RESPONSE** and **RECOVERY** activity.

State Governors could certainly activate such units during man-made cyber disasters and to support response and recovery operations in natural disasters, as well as provide support to the U.S. Department of Homeland Security missions. However, only a handful of such states have these elite cyber warfare units.

Integration with the Whole Community Concept

The Whole Community Approach to Preparedness promoted by Presidential Policy Directive 8 (**PPD-8**: National Preparedness) is a comprehensive and integrated approach to community preparedness for disasters – to include man made cyber events and their cascading consequences.

The increased interaction of public safety agencies and private entities with these National Guard cyber units in support of **PPD-8** should be addressed by the Pentagon. Alignment of Guard cyber capabilities to jointly respond with other Whole Community partners in a realistic approach to a CIKR cyber event (and the associated potential downstream effects on public utilities, medical facilities, transportation arteries, etc.) should be planned for.

Joint planning would help define how these Guard units could more effectively interface with other response agencies during cyber events and disasters. This would give Congress the Cyber Militia capability they are searching.

About the author: Dave Sweigert holds certifications as a Certified Information Systems Security Professional, Certified Information Systems Auditor, and Project Management Professional. He has earned Master's degrees in Information Security and Project Management. An Air Force veteran, he is a practitioner of cybersecurity, incident management and CIKR protection. He has consulted to Kaiser Permanente, J2 Global, NASA and the U.S. Army.